

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208921

(43)Date of publication of application : 26.07.2002

(51)Int.Cl.

H04L 9/08  
G06F 15/00  
H04L 9/32

(21)Application number : 2001-151279

(71)Applicant : NIPPON TELEGRAPH &  
TELEPHONE EAST CORP  
HITACHI SYSTEMS & SERVICES  
LTD

(22)Date of filing : 21.05.2001

(72)Inventor : ENDO HISASHI  
SHIBAYAMA HIROKO  
OKADA KENICHI  
KOSAKA TATSUYA  
GENDA KOICHI  
UENO KEIJI

(30)Priority

Priority number : 2000340853

Priority date : 08.11.2000

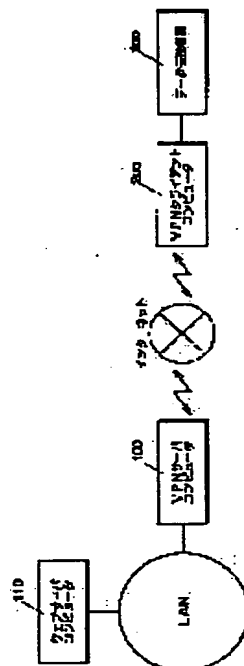
Priority country : JP

## (54) VPN DATA COMMUNICATION METHOD AND PRIVATE NETWORK CONSTRUCTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a VPN construction system which can construct a VPN without restriction by an IP address and access to a VPN server.

SOLUTION: In a portable data transmission device 300, a coding key used for coding treatment by a VPN client 200, a decoding key specific information for specifying a decoding key for decoding data coded by the VPN client 200, if received by a VPN server 100, and VPN transmission base data including an IP address of a VPN server are stored. The VPN client 200 reads transmission foundation data and stores it in a memory when the data transmission device 300 is connected. Thereby, transmission base data is not transferred on internet and data transmission is possible while keeping privacy.



## LEGAL STATUS

[Date of request for examination]

22.05.2001

[Date of sending the examiner's decision of rejection]

07.03.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-05938

[Date of requesting appeal against examiner's decision of rejection] 06.04.2005

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-208921

(P2002-208921A)

(43) 公開日 平成14年7月26日 (2002.7.26)

| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I           | テーマコード (参考)       |
|---------------------------|-------|---------------|-------------------|
| H 0 4 L 9/08              |       | G 0 6 F 15/00 | 3 3 0 A 5 B 0 8 5 |
| G 0 6 F 15/00             | 3 3 0 | H 0 4 L 9/00  | 6 0 1 C 5 J 1 0 4 |
| H 0 4 L 9/32              |       |               | 6 7 3 D           |

審査請求 有 請求項の数13 O L (全 22 頁)

(21) 出願番号 特願2001-151279 (P2001-151279)

(22) 出願日 平成13年5月21日 (2001.5.21)

(31) 優先権主張番号 特願2000-340853 (P2000-340853)

(32) 優先日 平成12年11月8日 (2000.11.8)

(33) 優先権主張国 日本 (J P)

(71) 出願人 399040405

東日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(71) 出願人 391002409

株式会社 日立システムアンドサービス

東京都大田区大森北3丁目2番16号

(72) 発明者 遠藤 久

東京都新宿区西新宿三丁目19番2号 東日

本電信電話株式会社内

(74) 代理人 100092956

弁理士 古谷 栄男 (外2名)

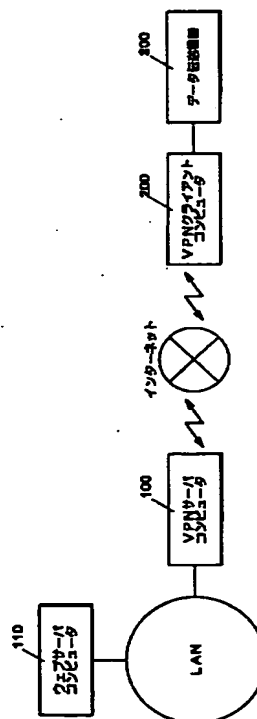
最終頁に続く

(54) 【発明の名称】 VPNデータ通信方法および私設網構築システム

(57) 【要約】

【課題】 IPアドレスに拘束されず、かつ、VPNサーバにアクセスすることなく、VPNを構築できるVPN構築システムを提供する。

【解決手段】 携行可能なデータ伝送機器300は、VPNクライアント200にて暗号化処理に用いる暗号化キー、VPNクライアント200によって暗号化されたデータをVPNサーバ100が受信した場合に、これを復号化する復号化キーを特定する復号化キー特定情報、およびVPNサーバのIPアドレスを含むVPN伝送基礎データを記憶している。VPNクライアント200は、データ伝送機器300が接続されると、伝送基礎データを読み出してメモリに記憶する。インターネット上を伝送基礎データが転送されず、守秘性を保持しつつ、データ伝送が可能となる。



**【特許請求の範囲】**

【請求項1】 A) VPNサーバコンピュータとVPNクライアントコンピュータとの間で、ネットワークを介してVPNを構築してデータ通信する方法であって、

B) VPNクライアントコンピュータとの間でデータ伝送が可能で、かつ携帯可能なデータ伝送機器に、VPNクライアントコンピュータがVPNサーバコンピュータとの間でVPN伝送時に用いるVPN伝送基礎データであって、少なくとも1)VPNクライアントコンピュータにて暗号化処理に用いるVPN暗号化キーまたはVPN暗号化キーを特定するVPN暗号化キー特定情報、2)VPNサーバコンピュータで復号化処理に用いるVPN復号化キーを特定するVPN復号化キー特定情報、および3)VPNサーバコンピュータのIPアドレスを含むVPN伝送基礎データを記憶させておき、

C) 前記データ伝送機器をVPN構築希望するVPNクライアントコンピュータに接続し、

D) 前記データ伝送機器から前記VPN伝送基礎データを読み出して、前記VPNサーバコンピュータとの間で、VPNを構築し、前記VPNサーバコンピュータへデータ送信要求があると、送信対象データを前記VPN暗号化キーを用いて暗号化して、前記VPN復号化キー特定情報とともに前記VPNサーバコンピュータのIPアドレスにデータ転送し、

E) 前記VPNサーバコンピュータは、前記VPN復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理すること、を特徴とするVPNデータ通信方法。

【請求項2】 仮想私設網サーバコンピュータ、

ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータ、を備え、前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、

携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1)仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キー特定情報、2)仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、および3)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、

前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータと

の間で、仮想私設網を構築すること、を特徴とする仮想私設網構築システム。

【請求項3】 仮想私設網サーバコンピュータ、

ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータ、を備え、前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、

携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1)仮想私設網クライアントコンピュータと仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定する仮想私設網暗号化復号化キー特定情報、および2)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、

前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して、前記仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定することにより、仮想私設網を構築すること、

を特徴とする仮想私設網構築システム。

【請求項4】 請求項2または請求項3の仮想私設網システムにおいて、

前記仮想私設網クライアントコンピュータは、前記仮想私設網暗号化キーを用いて暗号化して、前記仮想私設網復号化キー特定情報とともに前記仮想私設網サーバコンピュータへデータ転送し、

前記仮想私設網サーバコンピュータは前記仮想私設網復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理すること、を特徴とするもの。

【請求項5】 仮想私設網サーバコンピュータとネットワークを介して接続された仮想私設網クライアントコンピュータであって、前記仮想私設網サーバコンピュータとの間で、受信した暗号化データを復号化できる復号化キーを記憶しておき、データ伝送する仮想私設網クライアントコンピュータにおいて、

携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも仮想私設網暗号化キー、仮想私設網復号化キー特定情報、および仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、

前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築すること、

を特徴とする仮想私設網クライアントコンピュータ。

【請求項6】コンピュータを、仮想私設網サーバコンピュータから受信した暗号化データを復号化できる復号化キーを記憶しておきネットワークを介して接続された仮想私設網サーバコンピュータとの間でデータ伝送する仮想私設網クライアントコンピュータとして機能させるためのコンピュータ可読のプログラムであって、以下の処理を実行する、

前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも仮想私設網暗号化キー、仮想私設網復号化キー特定情報、および仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶した携帯可能なデータ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する、ためのプログラムであることを特徴とするコンピュータ可読のプログラム。

【請求項7】クライアントコンピュータと特定のサーバコンピュータ又または特定のLANとの間の通信で、クライアントコンピュータ内部またはクライアントコンピュータとネットワークとの間にVPNクライアント機能を配備し、上記特定サーバ内部または特定サーバや特定LANとネットワークとの間にVPNサーバ機能を配備し、上記VPNクライアントとVPNサーバ機能との間で転送されるデータを暗号化して転送するVPN通信システムにおいて、

A) 上記ネットワークはインターネット等の公衆ネットワークやLANであり、

B) VPNクライアント機能は携帯可能なデータ伝送機器とデータ伝送機器を動作させるドライバプログラムから構成され、

C) VPNクライアント機能のドライバプログラムは、前記データ伝送機器をVPN通信するクライアントコンピュータに接続した時、前記データ伝送機器から前記VPN伝送基礎データをクライアントコンピュータに読み出し動作可能な状態とし、

D) 前記携帯可能なデータ伝送機器には、VPN伝送基礎データとして、d1) VPNクライアント識別情報、d2) 暗号化復号化処理に必要な暗号鍵情報、d3) VPNサーバ機能を示すIPアドレス、d4) 上記特定サーバを示すIPアドレスまたは特定LANを示すIPサブネットアドレスを内蔵し、

E) VPNサーバ機能には、VPNサーバ識別情報、暗号化通信するすべてのVPNクライアント識別情報、暗

号化復号化処理に必要な暗号鍵情報を内蔵し、

F) 前記VPNクライアント機能は、クライアントコンピュータが特定のサーバコンピュータまたは特定のLANへ向けてデータ送信する時、VPNサーバ機能との間でお互いのVPN伝送基礎データをやりとりすることによりVPNを確立し、送信対象データを前記VPN伝送基礎データを用いて暗号化し、前記VPNサーバ機能を示すIPアドレスにデータを転送し、

G) 前記VPNサーバ機能は、前記VPNクライアント機能と通信するためのVPN伝送基礎データに基づいて、前記暗号化されたデータを復号化する暗号鍵を用いて復号した後、前記特定のサーバコンピュータまたは特定のLANへデータを転送すること、を特徴とするVPN通信システム。

【請求項8】請求項2または請求項3の仮想私設網システムにおいて、

前記データ伝送機器には、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行すること、を特徴とするもの。

【請求項9】コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって、

前記コンピュータは、前記プログラムを記録した記録媒体が接続されると、

前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1) 仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キー特定情報、2) 仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、および3) 仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを、前記記録媒体から読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する、

ことを特徴とするコンピュータ可読のプログラムを記録した記録媒体。

【請求項10】請求項9のプログラムを記録した記録媒体において、

前記記録媒体には、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行すること、を特徴とするもの。

【請求項 11】請求項 10 のプログラムを記録した記録媒体において、

前記録媒体は、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データが記録された仮想私設網関連データ記憶部と、前記仮想私設網関連データを読み出すための読み出しプログラムが記録された読み出しプログラム記録部とを有しており、

前記仮想私設網関連データ記憶部は、前記クライアントコンピュータのファイルシステムとは異なるデータ構造で記録されており、

前記読み出しプログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データを読み出して、前記仮想私設網の構築を実行すること、

を特徴とするもの。

【請求項 12】データを記録した記録媒体を、コンピュータに接続することにより、前記コンピュータのオペレーティングシステムプログラムが、前記記録媒体に記録された仮想私設網構築プログラムを起動させ、かかる仮想私設網構築プログラムによって、前記記録媒体に記録された仮想私設網構築用データを読み出して、仮想私設網サーバコンピュータとの間で仮想私設網を構築する方法であって、

前記仮想私設網構築データは、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶されており、

前記仮想私設網構築プログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムであること、

ことを特徴とする仮想私設網を構築する方法。

【請求項 13】コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で仮想私設網を構築した仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって前記記録媒体には、

1) 前記仮想私設網構築データが前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記録されており、

2) 使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムが前記オペレーティングシステムプログラムが記録されているデータのデータ形式を離隔できる領域に記録されている、

ことを特徴とするプログラムを記録したコンピュータ可

読の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、VPN に関し、特に、コンピュータの IP アドレスに依存しない VPN クライアントコンピュータに関する。

【0002】

【従来技術】今日、パッチャルプライベートネットワーク（以下 VPN と略す）が注目されている。これは、ネットワークを介しても、守秘性の高いネットワークを個人単位で構築する技術である。図 14 を用いて、簡単に説明する。

【0003】A 社の会計処理サーバコンピュータ 500 には社内 LAN を介して VPN サーバコンピュータ 503 が接続されている。B 社の端末コンピュータ 603 には、VPN クライアントプログラムがインストールされている。VPN サーバコンピュータ 503 および端末コンピュータ 603 双方には、VPN を形成するための VPN データが記憶されている。端末の操作者は、VPN クライアントプログラムを実行して、VPN サーバコンピュータ 503 との間で、VPN を構築する命令を端末コンピュータ 603 に与える。端末コンピュータ 603 は、かかる命令を受けて、記憶されている VPN データを用いて、VPN サーバコンピュータ 503 との間で、仮想的に、ネットワークを構築する。具体的には、端末 503 と会計処理サーバコンピュータ 500 との間のデータのやりとりは、前記 VPN データに含まれる暗号化処理データを用いて、暗号化されて実行される。このように、予め登録されたコンピュータ間のデータ伝送を VPN サーバコンピュータを介して行うことにより、ネットワークを介しても、個人レベルで守秘性の高い伝送が可能となる。

【0004】

【発明が解決しようとする課題】しかしながら、VPN の構築には以下のような問題があった。例えば、前記端末コンピュータ 603 の操作者が、出張のために、別のコンピュータと会計処理サーバコンピュータ 500 との間で守秘性の高いデータ伝送をさせる場合には、予め当該コンピュータおよび会計処理サーバコンピュータ 500 に VPN データを記憶させておかなければならない。

【0005】かかる問題を解決するために、特開 2000-59357 号公報に開示されているように、各ユーザについて ID およびパスワードを記録した IC カードを発行し、前記 ID およびパスワードを用いて管理サーバコンピュータにアクセスし、VPN サーバコンピュータで用いる公開鍵および自己の秘密鍵を取得して、VPN 情報を取得して VPN を構築することも考えられる。しかし、これでは、VPN を構築する場合には、自己の秘密鍵がネットワーク上を転送されるので、自己の秘密鍵が第三者に取得されるおそれがある。特に、ネットワ

ークとしてインターネットというオープンなネットワークを介在させる場合に、より第三者への情報の漏れが問題となる。

【0006】また、VPNを構築する都度、管理サーバコンピュータにアクセスする必要がある、管理サーバコンピュータが混雑している場合には、VPN構築に時間がかかる。

【0007】この発明は、仮想私設網の構築情報について守秘性を保持しつつ、仮想私設網の対象となるコンピュータの柔軟性を向上させたネットワークを用いた仮想私設網を構築することができる仮想私設網構築システムを提供することを目的とする。さらに、簡易に仮想私設網を構築できる仮想私設網構築システムを提供することを目的とする。

【0008】

【課題を解決するための手段および発明の効果】1) 本発明にかかるVPNデータ通信方法においては、A) VPNサーバコンピュータとVPNクライアントコンピュータとの間で、ネットワークを介してVPNを構築してデータ通信する方法であって、B) VPNクライアントコンピュータとの間でデータ伝送が可能で、かつ携帯可能なデータ伝送機器に、VPNクライアントコンピュータがVPNサーバコンピュータとの間でVPN伝送時に用いるVPN伝送基礎データであって、少なくとも1) VPNクライアントコンピュータにて暗号化処理に用いるVPN暗号化キーまたはVPN暗号化キーを特定するVPN暗号化キー特定情報、2) VPNサーバコンピュータで復号化処理に用いるVPN復号化キーを特定するVPN復号化キー特定情報、および3) VPNサーバコンピュータのIPアドレスを含むVPN伝送基礎データを記憶させておき、C) 前記データ伝送機器をVPN構築希望するVPNクライアントコンピュータに接続し、D) 前記データ伝送機器から前記VPN伝送基礎データを読み出して、前記VPNサーバコンピュータとの間で、VPNを構築し、前記VPNサーバコンピュータへデータ送信要求があると、送信対象データを前記VPN暗号化キーを用いて暗号化して、前記VPN復号化キー特定情報とともに前記VPNサーバコンピュータのIPアドレスにデータ転送し、E) 前記VPNサーバコンピュータは、前記VPN復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理する。

【0009】このように、携帯可能なデータ伝送機器にVPN伝送基礎データを記憶させておき、VPN構築希望のVPNクライアントコンピュータに接続させて、VPNを構築することにより、予めVPN伝送基礎データを記憶させていないVPNクライアントコンピュータであっても、VPN構築が可能となる。また、前記データ伝送機器に暗号化キーを記憶させているので、VPNクライアントコンピュータで用いる暗号化キーがネットワ

ーク上を転送されることによるセキュリティ低下の問題もない。また、VPN復号化キー特定情報およびVPNサーバコンピュータのIPアドレスを記憶しているので、VPNサーバコンピュータにアクセスすることなく、VPNを構築することができる。

【0010】2) 本発明にかかる仮想私設網システムにおいては、A) 仮想私設網サーバコンピュータ、B) ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータを備え、C) 前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、D) 携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくともd1) 仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キーを特定する仮想私設網暗号化キー特定情報、d2) 仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、およびd3) 仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、E) 前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する。

【0011】このように、携帯可能なデータ伝送機器に仮想私設網伝送基礎データを記憶させておき、仮想私設網構築希望の仮想私設網クライアントコンピュータに接続させて、仮想私設網を構築することにより、予め仮想私設網伝送基礎データを記憶させていない仮想私設網クライアントコンピュータであっても、仮想私設網構築が可能となる。また、前記データ伝送機器に暗号化キーを記憶させているので、ネットワーク上を暗号化キーが転送されることによるセキュリティ低下の問題もない。また、仮想私設網復号化キー特定情報および仮想私設網サーバコンピュータのコンピュータ特定データを記憶しているため、仮想私設網サーバにアクセスすることなく、仮想私設網を構築することができる。

【0012】3) 本発明にかかる仮想私設網システムにおいては、A) 仮想私設網サーバコンピュータ、B) ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータを備え、C) 前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、D) 携帯可能なデータ伝送機器に、前記仮想私

設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくともd1) 仮想私設網クライアントコンピュータと仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定する仮想私設網暗号化復号化キー特定情報、およびd2) 仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、E) 前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して、前記仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定することにより、仮想私設網を構築する。

【0013】このように、携帯可能なデータ伝送機器に仮想私設網伝送基礎データを記憶させておき、仮想私設網構築希望の仮想私設網クライアントコンピュータに接続させて、仮想私設網を構築することにより、予め仮想私設網伝送基礎データを記憶させていない仮想私設網クライアントコンピュータであっても、仮想私設網構築が可能となる。また、前記データ伝送機器に暗号化キーを特定する特定情報を記憶させているので、ネットワーク上を暗号化キーが転送されることによるセキュリティ低下の問題もない。

【0014】4) 本発明にかかる仮想私設網システムにおいては、前記仮想私設網クライアントコンピュータは、前記仮想私設網サーバコンピュータへのデータ送信要求があると、送信対象データを前記仮想私設網暗号化キーを用いて暗号化して、前記仮想私設網復号化キー特定情報とともに前記仮想私設網サーバへデータ転送し、前記仮想私設網サーバコンピュータは、前記仮想私設網復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理する。これにより、VPNを用いたデータ通信が可能となる。

【0015】5) 本発明にかかる仮想私設網クライアントコンピュータにおいては、A) 仮想私設網サーバコンピュータとネットワークを介して接続された仮想私設網クライアントコンピュータであって、前記仮想私設網サーバコンピュータとの間で、受信した暗号化データを復号化できる復号化キーを記憶しておき、データ伝送する仮想私設網クライアントコンピュータであって、B) 携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくともb1) 仮想私設網暗号化キーまたは仮想私設網暗号化キーを特定する仮想私設網暗号化キー特定情報、b2) 仮想私設網復号化キー特定情報、およびb3) 仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを

記憶させておき、C) 前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する。

【0016】このように、携帯可能なデータ伝送機器に仮想私設網伝送基礎データを記憶させておき、仮想私設網構築希望の仮想私設網クライアントコンピュータに接続させて、仮想私設網を構築することにより、予め仮想私設網伝送基礎データを記憶させていない仮想私設網クライアントコンピュータであっても、仮想私設網構築が可能となる。また、前記データ伝送機器に暗号化キーを記憶させているので、ネットワーク上を暗号化キーが転送されることによるセキュリティ低下の問題もない。また、仮想私設網復号化キー特定情報および仮想私設網サーバコンピュータのコンピュータ特定データを記憶しているので、仮想私設網サーバにアクセスすることなく、仮想私設網を構築することができる。

【0017】7) 本発明にかかるVPN通信システムにおいては、クライアントコンピュータと特定のサーバコンピュータ又または特定のLANとの間の通信で、クライアントコンピュータ内部またはクライアントコンピュータとネットワークとの間にVPNクライアント機能を配備し、上記特定サーバ内部または特定サーバや特定LANとネットワークとの間にVPNサーバ機能を配備し、上記VPNクライアントとVPNサーバ機能との間で転送されるデータを暗号化して転送するVPN通信システムにおいて、A) 上記ネットワークはインターネット等の公衆ネットワークやLANであり、B) VPNクライアント機能は携帯可能なデータ伝送機器とデータ伝送機器を動作させるドライバプログラムから構成され、C) VPNクライアント機能のドライバプログラムは、前記データ伝送機器をVPN通信するクライアントコンピュータに接続した時、前記データ伝送機器から前記VPN伝送基礎データをクライアントコンピュータに読み出し動作可能な状態とし、D) 前記携帯可能なデータ伝送機器には、VPN伝送基礎データとして、d1) VPNクライアント識別情報、d2) 暗号化復号化処理に必要な暗号鍵情報、d3) VPNサーバ機能を示すIPアドレス、d4) 上記特定サーバを示すIPアドレスまたは特定LANを示すIPサブネットアドレスを内蔵し、E) VPNサーバ機能には、VPNサーバ識別情報、暗号化通信するすべてのVPNクライアント識別情報、暗号化復号化処理に必要な暗号鍵情報を内蔵し、F) 前記VPNクライアント機能は、クライアントコンピュータが特定のサーバコンピュータまたは特定のLANへ向けてデータ送信する時、VPNサーバ機能との間でお互いのVPN伝送基礎データをやりとりすることによりVPNを確立し、送信対象データを前記VPN伝送基礎データを用いて暗号化し、前記VPNサーバ機能を示すIPアドレスにデータを転送し、G) 前記VPNサーバ機能は、



前記VPNクライアント機能と通信するためのVPN伝送基礎データに基づいて、前記暗号化されたデータを復号化する暗号鍵を用いて復号した後、前記特定のサーバコンピュータまたは特定のLANへデータを転送する。

【0018】このように、携帯可能なデータ伝送機器にVPN伝送基礎データを記憶させておき、VPN構築希望のクライアントコンピュータに接続させてVPNを構築することにより、クライアントコンピュータがVPN通信に必要な暗号鍵がネットワーク上を転送されることによるセキュリティ低下の問題がない。またVPN伝送基礎データを携帯しているため、VPN通信のたびにVPNクライアント機能からVPNサーバ機能にアクセスする必要がなく、VPNサーバ機能の処理負荷を低減できる。

【0019】8) 本発明にかかる仮想私設網システムにおいては、前記データ伝送機器には、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行する。したがって、前記仮想私設網クライアントコンピュータ用のプログラムが記録されていないコンピュータであっても、前記データ伝送機器を接続するだけで、仮想私設網クライアントコンピュータとして機能させることができる。

【0020】9) 本発明にかかる記録媒体においては、コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって、前記コンピュータは、前記プログラムを記録した記録媒体が接続されると、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1) 仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キー特定情報、2) 仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、および3) 仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを、前記記録媒体から読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する。したがって、前記仮想私設網伝送基礎データを有していないコンピュータであっても、前記データ伝送機器を接続すれば、仮想私設網を構築することができる。

【0021】10) 本発明にかかる記録媒体においては、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコン

ピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行する。したがって、前記仮想私設網クライアントコンピュータ用のプログラムが記録されていないコンピュータであっても、前記データ伝送機器を接続するだけで、仮想私設網クライアントコンピュータとして機能させることができる。

【0022】11) 本発明にかかる記録媒体においては、前記記録媒体は、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データが記録された仮想私設網関連データ記憶部と、前記仮想私設網関連データを読み出すための読み出しプログラムが記録された読み出しプログラム記録部とを有しており、前記仮想私設網関連データ記憶部は、前記クライアントコンピュータのファイルシステムとは異なるデータ構造で記録されている。前記読み出しプログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データを読み出して、前記仮想私設網の構築を実行する。このように、仮想私設網伝送基礎データを前記コンピュータのファイルシステムとは異なるデータ構造で記録しておき、前記読み出しプログラムを介して、仮想私設網伝送基礎データおよび仮想私設網クライアントコンピュータ用のプログラムを読み出すことにより、仮想私設網伝送基礎データおよびそのプログラムの盗み見ることから防止することができる。特に、仮想私設網クライアントコンピュータ用のプログラムを前記記録媒体に記録する場合には、かかる直接読み取りできなくすることにより、より守秘性を高めることができる。

【0023】11) 本発明にかかる仮想私設網を構築する方法においては、データを記録した記録媒体を、コンピュータに接続することにより、前記コンピュータのオペレーティングシステムプログラムが、前記記録媒体に記録された仮想私設網構築プログラムを起動させ、かかる仮想私設網構築プログラムによって、前記記録媒体に記録された仮想私設網構築用データを読み出して、仮想私設網サーバコンピュータとの間で仮想私設網を構築する方法であって、前記仮想私設網構築データは、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶されており、前記仮想私設網構築プログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムである。このように、前記仮想私設網構築データを、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶しておき、前記仮想私設網構築プログラムが前記仮想私設網構築データを読み出

すことにより、前記仮想私設網構築データを盗み見ることから防止することができる。特に、仮想私設網クライアントコンピュータ用のプログラムを前記記録媒体に記録する場合には、かかる直接読み取りできなくすることにより、より守秘性を高めることができる。

【0024】12) 本発明にかかるプログラムを記録したコンピュータ可読の記録媒体においては、コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で仮想私設網を構築した仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって、前記記録媒体には、1) 前記仮想私設網構築データが前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記録されており、2) 利用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムが前記オペレーティングシステムプログラムが記録されているデータのデータ形式を離隔できる領域に記録されている。このように、前記仮想私設網構築データを、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶しておき、前記仮想私設網構築プログラムが前記仮想私設網構築データを読み出すことにより、前記仮想私設網構築データを盗み見ることから防止することができる。特に、仮想私設網構築プログラムを前記記録媒体に記録して、当該記録媒体さえあれば、仮想私設網を構築できるようにする場合には、かかる直接読み取りできなくすることにより、より守秘性を高めることができる。

【0025】なお、VPNサーバ機能からVPNクライアント機能への通信も逆の手順で同様にすればよい。

【0026】本実施形態においては、仮想私設網復号化キー特定情報として、VPNサーバ識別子およびVPNクライアント識別子を用いた。これにより、1つのVPNサーバについて、複数のVPNサーバ識別子を設定することができる。しかし、仮想私設網復号化キー特定情報としては、VPNサーバに記憶された復号化キーのうち、いずれを用いて復号すればよいかを特定できるものであればどのようなものであってもよく、復号化キー番号などであってもよい。この場合には、VPNサーバ識別子は不要となる。

【0027】また、VPN暗号化方式は1つの方式に決めておけば、VPN伝送基礎データに記憶させる必要はない。

【0028】なお、「読み出しプログラム」とは、実施形態では、起動プログラム411aが該当する。「利用者識別情報」とは、実施形態ではIDとパスワードが該当する。また、「仮想私設網関連データ記憶部」「読み出しプログラム記録部」は、それぞれ、領域412、領

域411に該当する。また、「隠しデータ領域」とは実施形態では領域412に該当する。

#### 【0029】

【発明の実施の形態】1. 概略および機能ブロックの説明

本発明の一実施形態を図面に基づいて説明する。図1に示す仮想私設網データ伝送システムは、VPNサーバコンピュータ（以下VPNサーバと略す）100、VPNクライアントコンピュータ（以下VPNクライアントと略す）200およびデータ伝送機器300を備えている。

【0030】VPNサーバ100は、LANでウェブサーバコンピュータ110に接続されている。VPNクライアント200はインターネットなどのネットワークを介してVPNサーバ100に接続されている。VPNクライアント200には、データ伝送機器300が接続されている。

【0031】本システムの主要部分の詳細機能ブロックについて、図2を用いて説明する。

【0032】データ伝送機器300は、送受信手段11、判定手段12、VPN伝送基礎データ記憶手段10を備えている。

【0033】VPN伝送基礎データ記憶手段10は、VPN伝送基礎データを記憶する。VPN伝送基礎データは、少なくとも、1) VPNクライアント200にて暗号化処理に用いるVPN暗号化キー、2) VPNクライアント200によって暗号化されたデータをVPNサーバ100が受信した場合に、これを復号化する時に用いるVPN復号化キーを特定するVPN復号化キー特定情報、および3) VPNサーバのIPアドレスを含む。

【0034】VPNクライアント200は、接続状態制御手段6、読み出しデータ記憶手段4、報知手段7および入力手段8を備えており、データ伝送機器300が接続されると、以下のようにして、前記VPN伝送基礎データ記憶手段10に記憶されたVPN伝送基礎データを読み出して、読み出しデータ記憶手段4に記憶する。

【0035】接続状態制御手段6は、データ伝送機器300が接続されるとこれを検出し、報知手段7によって、操作者に、操作者IDおよびパスワード入力可能状態であることを報知する。操作者は、操作者IDおよびパスワードを入力手段8から入力する。接続状態制御手段6は入力された操作者IDおよびパスワードをデータ伝送機器300の送受信手段11に送信する。送受信手段11は、これらの操作者IDおよびパスワードを判定手段12に与える。判定手段は与えられた操作者IDおよびパスワードが一致しているか否かを判断し、一致している場合には、一致判断信号を送受信手段11に与える。なお、判別手段が、IDおよびパスワードに換えて、操作者がデータ伝送機器の正当な使用者であることを判別するようにしてもよい。判別手法としては指紋、

声紋等を用いた判別が、採用可能である。

【0036】送受信手段11は、かかる一致判断信号を受けて、接続状態制御手段6にVPN伝送基礎データの読み出し許可信号を送信する。接続状態制御手段6はかかる読み出し許可信号を受け取ると、VPN伝送基礎データ取得要求を送受信手段11に出力する。送受信手段11はVPN伝送基礎データをVPN伝送基礎データ記憶手段10から読み出して、接続状態制御手段6に出力する。接続状態制御手段6は、与えられたVPN伝送基礎データを読み出しデータ記憶手段4に記憶させる。

【0037】かかる読み出しデータ記憶手段4への書き込みにより、VPNサーバ100との間でネットワークを介しても伝送対象データの守秘性を保持しつつ、データ伝送が可能となる。本明細書においては、かかる状態をVPNが構築されたと呼ぶ。

【0038】データ伝送について説明する。暗号化手段3は、処理手段2から暗号処理対象のデータを受け取ると、読み出しデータ記憶手段4に記憶されたVPN伝送基礎データのうちVPNクライアント200にて暗号化処理に用いるVPN暗号化キーを用いて暗号化し、VPNクライアント200によって暗号化されたデータをVPNサーバ100が受信した場合に、これを復号化する時に用いるVPN復号化キーを特定するVPN復号化キー特定情報とともに、VPNサーバ100のIPアドレスに転送する。

【0039】VPNサーバ100は、復号化手段15、VPN伝送基礎データ記憶手段14、暗号化手段13を備えている。復号化手段15は、前記VPN復号化キー特定情報に基づき、VPN伝送基礎データ記憶手段14に記憶された複数の復号化キーから復号処理に用いるキーを特定し、VPNクライアント200によって暗号化されたデータを復号化して、他のコンピュータへ出力する。

【0040】VPN伝送基礎データ記憶手段14は、VPNサーバ100にて暗号化処理に用いるVPN暗号化キー、およびVPNサーバ100によって暗号化されたデータをVPNクライアント200が受信した場合に、これを復号化する時に用いるVPN復号化キーを特定するVPN復号化キー特定情報を含むVPN伝送基礎データを記憶する。暗号化手段13は、VPN伝送基礎データ記憶手段14に記憶された暗号化キーを用いて、他のコンピュータから与えられたデータを暗号化して、VPN伝送基礎データ記憶手段14に記憶されたVPN復号化キー特定情報とともに、伝送データを受け取ったコンピュータのIPアドレス（この場合、VPNクライアント200のIPアドレス）に転送する。

【0041】VPNクライアント200の復号化手段5は、VPNサーバ100から受け取ったVPN復号化キー特定情報に基づき、読み出しデータ記憶手段4に記憶された復号化キーのうち復号処理に用いるキーを特定

し、VPNサーバ100によって暗号化されたデータを復号化して、処理手段2へ出力する。

【0042】なお、上記例では、VPNクライアント200からデータ伝送する場合について説明したが、VPNサーバ100からデータ伝送することも可能である。この場合の処理は同様であるので説明は省略する。

【0043】なお、VPNクライアントのIPアドレスについては、例えば、VPNクライアント200からVPNサーバ100にデータが伝送された時に取得できる。

【0044】また、VPNクライアントのIPアドレスを、予め、VPNサーバのVPN伝送基礎データ記憶手段に記憶しておくことにより、VPNサーバからのVPN伝送も可能である。

【0045】また、VPNクライアントとしてユーザに選択されるコンピュータの範囲が決定されている場合には、VPNサーバにVPNクライアントIPアドレスの候補を複数記憶しておいてもよい。この場合には、VPNサーバからVPNを構築することも可能となる。

【0046】また、上記実施形態においては、VPN伝送基礎データとして、VPN暗号化キー、VPN復号化キー特定情報、およびVPNサーバのIPアドレスを含む場合について説明したが、VPN暗号化キーについては、VPN暗号化キーを特定するためのVPN暗号化キー特定情報であってもよい。この場合、VPN暗号化キーを特定するためのプログラムを記憶しておき、VPNクライアント単独でまたはVPNサーバと連携してVPN暗号化キーを決定（生成）してもよい。

【0047】また、VPNクライアントのVPN伝送基礎データとして、少なくともVPNキー特定情報および対向するVPNサーバのIPアドレスを記憶しておき、VPNサーバと連携してVPN暗号化キーおよびVPN復号化キーを決定するようにしてもよい。なお、VPNサーバのVPN伝送基礎データとして、少なくともVPNキー特定情報および対向するVPNクライアントのIPアドレスを記憶しておき、VPNクライアントと連携してVPN暗号化キーおよびVPN復号化キーを決定するようにしてもよい。

【0048】かかるVPN暗号化キーおよびVPN復号化キーの生成については、例えば、IPSECの標準鍵交換方式のIKE (internet key exchange) を用いてもよい。

【0049】このようにして、非閉鎖的なネットワークを介しても、守秘性の高いデータ伝送が可能となるVPNが構築状態となる。

## 【0050】2. ハードウェア構成

図2に示すVPNサーバ100のハードウェア構成について図3を用いて説明する。図3は、VPNサーバ100をCPUを用いて構成したハードウェア構成の一例である。以下では、VPNの標準プロトコルとして、IPSec (Security Architectuer for Internet Protocol) の鍵

交換方式の1つである手動鍵方式を採用した場合について説明する。

【0051】VPNサーバ100は、CPU23、メモリ27、ハードディスク26、CRT30、CDD(CDROMドライブ)25、キーボード28、マウス31、ネットワーク管理部32およびバスライン29を備えている。CPU23は、ハードディスク26に記憶されたプログラムにしたがいバスライン29を介して、各部を制御する。なお、オペレーティングシステムとしては、例えば、ウインドウズNT(商標)等を採用すればよい。

【0052】ハードディスク26には、オペレーティングプログラム(OS)26o、VPNサーバプログラム26p、およびVPNデータ記憶部26dを有する。

【0053】これらのプログラムは、CDD25を介して、プログラムが記憶されたCDROM25aから読み出されてハードディスク26にインストールされたものである。なお、CDROM以外に、フレキシブルディスク(FD)、ICカード等のプログラムをコンピュータ可読の記録媒体から、ハードディスクにインストールさせるようにしてもよい。さらに、通信回線を用いてダウンロードするようにしてもよい。

【0054】本実施形態においては、プログラムをCDROMからハードディスク26にインストールさせることにより、CDROMに記憶させたプログラムを間接的にコンピュータに実行させるようにしている。しかし、これに限定されることなく、CDROMに記憶させたプログラムをCDD25から直接的に実行するようにしてもよい。なお、コンピュータによって、実行可能なプログラムとしては、そのままのインストールするだけで直接実行可能なものはもちろん、一旦他の形態等に変換が必要なもの(例えば、データ圧縮されているものを、解凍する等)、さらには、他のモジュール部分と組合して実行可能なものも含む。

【0055】VPNデータ記憶部26dのデータ構造について、図4を用いて説明する。VPNデータ記憶部26dには、VPNクライアント識別子、VPNサーバ識別子、VPN暗号化方式、VPN復号化キー、およびVPN暗号化キーが記憶されている。

【0056】VPNクライアント識別子およびVPNサーバ識別子は、VPNサーバとVPNクライアントとの間で暗号化されて伝送されるデータについて、いずれのデータを用いて復号すればよいかを決定するためのVPN復号化キー特定情報である。詳しくは後述する。VPN復号化キーは、VPNクライアントにおいて暗号化されたデータをVPNサーバにて復号するためのキーである。VPN暗号化方式とは、VPNクライアントおよびVPNサーバにおいて暗号化する暗号化方式を示すデータである。VPN暗号化キーは、このVPNクライアントに伝送する場合の暗号化キーである。

【0057】たとえば、VPNクライアント識別子「AC101」、VPNサーバ識別子「AS105」、VPN暗号化方式「xxx1」、VPN復号化キー「595xxx5」、VPN暗号化キー「325yyy7」であれば、VPNクライアント識別子「AC101」からVPNサーバ識別子「AS105」宛に伝送されたデータは、VPN復号化キー「595xxx5」を用いてVPN暗号化方式「xxx1」で復号化される。また、VPNクライアント識別子「AC101」へのVPNサーバ識別子「AS105」から伝送されるデータは、VPN暗号化キー「325yyy7」を用いてVPN暗号化方式「xxx1」で暗号化される。

【0058】このように、VPNサーバ100には、VPNクライアントとの間でのVPN伝送方法を特定するデータが複数記憶されている。

【0059】ネットワーク管理部32はトラスト側(内部LAN側)とアントラスト側(インターネット側)のデータを区別して送受信することができる。

【0060】また、VPNプログラム26pについては後述する。

【0061】図2に示すVPNクライアント200のハードウェア構成について図5を用いて説明する。VPNクライアント200は、VPNサーバ100とハードウェア構成はほぼ同じであるが、さらにUSBIF133を有している。USBIF133は、USB(universal serial bus)のインターフェイスである。また、ハードディスク126に記憶されているデータが異なり、VPNクライアントプログラム126sおよびアプリケーションプログラム126aを有する。

【0062】各プログラムについては後述する。

【0063】図2に示すデータ伝送機器300のハードウェア構成について図6を用いて説明する。データ伝送機器300は、CPU223、ROM225、フラッシュメモリ227、パスワード判定部233、USBIF232およびバスライン229を備えている。本実施形態においては、データ伝送機器300としてVPNクライアント200に設けられたUSB端子(図示せず)にUSBプラグを挿入することにより、VPNクライアント200との間で内部に有するデータをデータ伝送可能なUSB機器(USBキー)を採用した。ROM225には外部との通信および各部を制御する制御プログラムが記録されている。フラッシュメモリ227には、VPNデータ記憶領域228を有している。VPNデータ記憶領域228について、図7を用いて説明する。VPNデータ記憶領域228には、ユーザID、パスワード、使用期限、VPNサーバのIPアドレス、相手先サーバのIPアドレス、VPN暗号化方式、VPN暗号化キー、VPN復号化キー、VPNクライアント識別子、およびVPNサーバ識別子が記憶されている。相手先サーバは例えば、ウェブサーバを示す。

【0064】ユーザIDおよびパスワードは、このデータ伝送機器300を使用許可が与えられているユーザであることを判別するためのデータである。使用期限は、このデータ伝送機器300を使用できる期限を表す。VPNサーバのIPアドレスは、VPN暗号化方式およびVPN暗号化キーによって、暗号化したデータを転送先であり、相手先サーバのIPアドレスは、VPNサーバによって復号化されたデータの転送先を示す。VPN復号化キーは、VPNサーバから与えられた暗号化されたデータを復号化する場合のキーである。VPNクライアント識別子およびVPNサーバ識別子は、VPNサーバとの間で相対的に決定された2つのコンピュータの識別子である。この点は、VPNサーバと同様である。

【0065】パスワード判定部233は与えられたIDおよびパスワードがあらかじめ記憶されているIDおよびパスワードと一致するか否かをハードウェアロジックで判断し、一致する場合には一致判断信号を出力し、一致しない場合には不一致判断信号を出力する。

### 【0066】3. フローチャート

以下では、既に述べたように、VPNの標準プロトコルとして、IPSecの鍵交換方式の1つである手動鍵方式を採用した場合について説明する。

【0067】図8～図11を用いて、VPNサーバ100とVPNクライアント200におけるVPNを用いたデータ伝送処理について説明する。以下では、図5に示すようなアプリケーションプログラム26aに基づいて出力されたデータを、VPNサーバ100に暗号化したまま送信し、図1に示すVPNサーバ100にLAN接続されたウェブサーバ110に復号化したデータとして転送する場合を例として説明する。

【0068】まず、図8を用いてVPNの構築処理について説明する。データ伝送機器300とVPNクライアント200との間で、以下のようにして、VPN基礎データが読み出され、メモリ127に書き込まれる。

【0069】まず、ユーザはデータ伝送機器300をVPNクライアント200のUSB端子に挿入する。VPNクライアント200は、OS126oに基づいて、自己のUSB端子（図示せず）にデータ伝送機器300が挿入されるか否かを検出しており、挿入を検出すると、使用期限内か否かを判断し、使用期限内であれば、当該ユーザがデータ伝送機器300の使用を許可されたユーザであるか否かを判断するために、ユーザIDおよびパスワードの入力画面を表示する（図8ステップS1）。ユーザは、キーボード128からユーザIDおよびパスワードを入力する。

【0070】CPU123は、ユーザIDおよびパスワードの入力があるか否かを判断しており（ステップS3）、ユーザIDおよびパスワードの入力があると、データ伝送機器300へ入力されたユーザIDおよびパスワードをUSBIF132を介して送信する（ステップ

S5）。

【0071】データ伝送機器300のCPU223は、USBIF232を介してユーザIDおよびパスワードを受信するか否かを判断しており（ステップS21）、かかるデータを受信すると、パスワード判定部233（図6参照）に受信したユーザIDおよびパスワードを与える（ステップS23）。パスワード判定部233は、既に説明したように、入力されたユーザIDおよびパスワードと、予め記録されているユーザIDおよびパスワードとが一致する場合には、一致信号を出力し、一致しない場合には、不一致信号を出力する。CPU223は、パスワード判定部233から一致信号が与えられるか否かを判断しており（ステップS25）、一致信号が与えられるとVPNクライアント200にUSBIF232を介して一致信号を送信する（ステップS27）。

【0072】VPNクライアント200のCPU123は、USBIF132を介して一致信号を受信するか否かを判断しており（ステップS7）、一致信号を受信するとデータ伝送機器300に記憶されたVPN伝送基礎データを取得するための要求命令を、USBIF132を介してデータ伝送機器300に送信する（ステップS9）。

【0073】データ伝送機器300のCPU223は、USBIF232を介して前記要求命令が与えられるか否かを判断しており（ステップS31）、前記要求命令が与えられると、VPNデータ記憶領域に記憶されたデータを、USBIF232を介して、VPNクライアント200に送信する（ステップS33）。

【0074】VPNクライアント200のCPU123は、応答があるか否かを判断しており（ステップS11）、応答があるとメモリ127に受信したVPN伝送基礎データを書き込む（ステップS13）。

【0075】かかるVPN伝送基礎データのメモリ127への書き込みにより、後述するようにVPNを用いた伝送が可能な状態となる。本明細書では、これを、VPNが構築されたと呼ぶ。

【0076】なお、ステップS25にて、不一致信号を受け取ると、CPU223は、USBIF232を介してVPNクライアント200に不一致信号を送信する（ステップS35）。クライアント200のCPU123は、ステップS7にて不一致信号を受信し、例えば、「ユーザIDまたはパスワードが違います。正しいユーザIDおよびパスワードを入力してください。」とアラームメッセージを表示する（ステップS15）。そして、ステップS1以下の処理を繰り返す。

【0077】VPNクライアント200とVPNサーバ100との間の伝送処理は、従来のVPNを用いた伝送と基本的には同じである。以下、図9を用いて、VPNを用いた伝送処理について説明する。

【0078】VPNクライアント200のCPU123

は、伝送対象のパケットのヘッダに記載された、伝送先コンピュータのIPアドレスを参照して、内部から外部への送信要求があるか否かを判断する（図9ステップS41）。この場合、アプリケーションプログラム26aに基づいて出力されたデータを、図1に示すウェブサーバ110に伝送する場合であるので、伝送対象のパケットのヘッダに記載されたウェブサーバ110のIPアドレスを参照して、かかる判断を実行する。

【0079】つぎに、CPU123は、送信先がVPNを用いた伝送を実行する送信先か否かを判断する（ステップS43）。これは、伝送対象パケットのヘッダ情報を参照して、伝送先コンピュータのIPアドレスが、メモリ127に読み出されているVPN伝送基礎データの相手先サーバのIPアドレスと一致するか否かを判断すればよい。

【0080】一致する場合は、CPU123は、VPN伝送基礎データを用いて暗号化して送信する（ステップS45）。具体的には、伝送対象のパケットをVPN暗号化キーを用いてVPN暗号化方式で暗号化し、パケット化する。このパケットのヘッダにこのパケットの伝送先であるVPNサーバのIPアドレス、VPNクライアント識別子、およびVPNサーバ識別子をヘッダに埋め込んで、送信する。なお、通常の送信と同様に、送信元であるVPNクライアント200のIPアドレスもヘッダに埋め込まれる。一方、ステップS43にて、一致しない場合は、VPNを用いた伝送ではないので、伝送対象パケットを破棄する（ステップS47）。なお、指定されたIPアドレスのコンピュータに暗号化することなく送信するようにしてもよい。この場合、ステップS45にて暗号化することなく、送信するようにすればよい。

【0081】VPNサーバ100のCPU23は、外部から内部への要求（リクエスト）を受信したか否かを判断している（ステップS61）。なお、外部からの要求であるか否かは、ネットワーク管理部のアントラスト側へ与えられたか否かを判断すればよい。内部への要求であるかは、伝送パケットのヘッダに自己のIPアドレスが転送先として指定されているか否かを判断すればよい。

【0082】外部から内部への要求を受信すると、CPU23は、指定先が図4に示すVPNデータ記憶部のデータリスト中に存在するか否かを判断する（ステップS63）。具体的には、ヘッダに存在するVPNクライアント識別子およびVPNサーバ識別子を検索キーとして、リストに存在するか否かを判断する。この場合、リストに存在するので、ヘッダ中から送信元であるVPNクライアント200のIPアドレスを読み出して、直前VPNクライアントIPアドレスをそのIPアドレスに書き換える（ステップS64）。この場合、ヘッダ情報として、VPNクライアント識別子「AC101」および

VPNサーバ識別子「AS105」が読み出され、図4に示すリストに存在するので、送信元のVPNクライアント200のIPアドレスを直前VPNクライアントIPアドレスに書き換える。このように、VPN復号化キー特定情報に対応づけてVPNクライアントIPアドレスを記憶しておくことにより、VPNクライアントIPアドレスが動的に変化する場合でも、VPNを用いたデータ通信が可能となる。

【0083】CPU23は、VPN復号化キーを特定して暗号化方式に則って復号化し、復号化後のデータから、転送先のサーバのIPアドレスを抽出し、当該IPアドレスのサーバに転送する（ステップS65）。この場合、対応するVPN復号化キー「595xxx5」を用いて、VPN暗号化方式で復号化する。復号化後のデータのヘッダ情報を参照すると、このパケットの相手先サーバのIPアドレスが、「202.xxx.xxx」であることがわかるので、かかるコンピュータに復号化したパケットを伝送する。

【0084】このように、ヘッダ情報に埋め込まれたVPNクライアント識別子およびVPNサーバ識別子は、VPNサーバ100にて伝送されたパケットを復号化する場合の復号化キーを特定するデータとして機能する。

【0085】伝送先のウェブサーバ110でデータ処理が実行されて、VPNクライアント200に応答を伝送する場合、次のように実行される。

【0086】VPNサーバ100のCPU23は、内部から外部への要求を受信したか否かを判断している（ステップS71）。なお、内部からの要求であるか否かは、ネットワーク管理部のトラスト側へ与えられたか否かを判断すればよい。したがって、ウェブサーバ110からVPNクライアント200への伝送データを受け取ると、送信先がVPNリストに存在するか否かを判断する（ステップS73）。この場合、この伝送データの送信先として、ウェブサーバ110は、自己が受信した要求発信元として指定されたIPアドレスが、直前VPNクライアントIPアドレスとして記憶されているか否かを判断すればよい。

【0087】この場合、送信先がVPNリストに存在するので、該当するVPN暗号化キー、VPN暗号化方式を用いて、暗号化して、直前VPNクライアントIPアドレスに送信する（ステップS75）。このとき、ヘッダ情報に、VPNクライアント識別子およびVPNサーバ識別子を埋め込む。かかるデータを埋め込むのは、VPNクライアント200にて伝送されたパケットを復号化する場合の復号化キー特定するためである。なお、ステップS75にて暗号化することなく、送信するようにしてもよい。

【0088】VPNクライアント200のCPU123は、外部から内部への要求（リクエスト）を受信したか否かを判断している（ステップS51）。これは、伝送対

象パケットのヘッダ情報に記憶された送信元のVPNサーバのIPアドレスおよび送信先のVPNクライアントのIPアドレスから判断すればよい。

【0089】CPU123は、メモリ127に読み出しているVPN伝送基礎データで復号すべきか否かを判断する(ステップS53)。具体的には、伝送対象パケットのヘッダ情報に存在するVPNクライアント識別子およびVPNサーバ識別子が、メモリ127に読み出しているVPN伝送基礎データのVPNクライアント識別子およびVPNサーバ識別子と一致するか否かを判断すればよい。

【0090】この場合、一致するので、メモリ127に読み出しているVPN伝送基礎データのVPN復号化キーを用いて、復号化し、アプリケーションプログラムに渡す(ステップS55)。以下、かかる処理を繰り返す。

【0091】なお、ステップS53にて一致しない場合には、VPNを用いた伝送ではないので破棄する(ステップS57)。なお、ステップS75にて暗号化されないで送信された場合には、ステップS55にて、復号化することなくアプリケーションプログラムに渡すようにすればよい。

【0092】本実施形態においては、VPNクライアントのIPアドレスが固定的ではない。したがって、図9ステップS64において、図4に示すリストに存在する場合には、直前VPNクライアントIPアドレスとして記憶するようにしている。これにより、VPNクライアントのIPアドレスに拘束されず、自由にVPNを構築することができる。また、VPNクライアント200にて、データ伝送機器300が取り外された場合には、VPNクライアント200のメモリから、読み出されたVPN伝送基礎データを消去するだけで、VPNサーバにはデータ伝送機器300が取り外されたことを送信しない。この場合でも、つぎに、同じまたは異なるコンピュータをVPNクライアントとしてVPN伝送がなされると、動的に前記VPNクライアントのIPアドレスを記憶するので、確実に、VPNクライアントのIPアドレスに拘束されないVPNを構築することができる。

【0093】なお、図9ステップS73にて、リストに存在しない場合は、VPNを用いた伝送ではないので破棄(無視)する(ステップS77)。

【0094】VPN切断処理について図10を用いて説明する。VPNクライアント200のCPU123は、OS1260に基づき、USB端子の接続状態が変化するか否かを判断している。VPNクライアント200のCPU123は、図10に示すプログラムを実行しており、「USB端子からデータ伝送機器が取り外された」との検出結果を受けるか否かを判断しており(ステップS81)、USB端子からデータ伝送機器300が取り外されると、メモリ127のVPN伝送基礎データを消

去する(ステップS83)。これにより、VPN伝送が不可能な状態となる。これを、VPN切断状態という。

【0095】このように、VPN伝送基礎データを携帯可能な接続機器に記録しておき、必要な端末に挿入することにより、コンピュータのIPアドレスに拘束されないVPNを構築することができる。また、接続機器を取り外すことにより、自動的にVPN伝送基礎データが消去されるので、当該コンピュータにて第三者がこのVPNを用いた伝送をすることを確実に防止することができる。

#### 【0096】4. 他の実施形態

なお、本実施形態においては、伝送機器としてUSBキーを用いたが、クライアントコンピュータとの間で内部に記憶されているデータのやりとりができるものであればどのようなものであってもよく、コンパクトフラッシュ(登録商標)、PCカード等の記録媒体を採用してもよい。また、コンピュータに設けられた端子に有線で接続する場合だけでなく、赤外線データ通信(例えば、IrDA(Infrared Data Association)規格など)やBluetoothなどで接続することも可能である。

【0097】また、データ伝送機器の発行および記録データの変更については、別途発行処理管理コンピュータを設ければよい。また、IDおよびパスワードを入力することにより、VPNクライアントで編集可能としてもよい。

【0098】なお、RSAなどの公開鍵形式で暗号化および復号化をする場合には、VPNサーバ100の公開鍵については、データ伝送機器300のVPN伝送基礎データ記憶手段10に記憶しておく必要はなく、暗号化するときに、VPNサーバ100にアクセスして取得するようにしてもよい。VPNクライアント200の公開鍵についても同様である。

【0099】本実施形態においては、VPN伝送基礎データを全てデータ伝送機器に格納して持ち歩くようにしている。これにより、VPNサーバからVPN伝送基礎データを転送させる必要がないので、守秘性を高めることができる。しかし、VPN伝送基礎データを全てデータ伝送機器に格納させるのではなく、その一部を格納させておき、残りのデータはVPNサーバからダウンロードするようにしてもよい。この場合、データの分割の仕方としては、合体させて初めてデータとして意義があるように、分割すればよい。たとえば、VPN暗号キーが12バイトから構成されている場合、前半の6バイトをデータ伝送機器に、後半の6バイトをVPNサーバから転送させて、両者を合体させて初めてVPN暗号キーがわかるようにすればよい。他の項目データについても同様である。この場合、分割の割合については、限定されない。

【0100】また、上記実施形態においては、図5に示すように、VPNクライアント11のハードディスクに

VPNプログラム126cをインストールしている場合について説明したが、VPNプログラムについては、フラッシュメモリチップおよびコントローラチップを搭載したコンパクトフラッシュ（CF）等の記録媒体に格納し、かかる記録媒体からプログラムを読み出すようにしてもよい。これにより、VPNプログラムを予めインストールしていないコンピュータであっても、VPN通信が可能となる。以下、図5に示すVPNクライアントで記述しているVPNプログラムをデータ伝送機器に内蔵した場合の実施形態について、説明する。

【0101】図11に、VPNクライアントとしてPDA（Personal Digital Assistants）を採用した場合の、ハードウェア構成を示す。このように、PDA400はCFスロット433を有しており、CFスロット433には後述するコンパクトフラッシュ433aが挿入される。ROM425にはオペレーティングシステムプログラム（OS）が記憶されている。

【0102】コンパクトフラッシュ433aのデータ構造を図12を用いて説明する。コンパクトフラッシュ433aは、PDA400のCPU423がOSによって認識できる領域と、認識できない領域に分割されている。これにより、VPN個人情報等のVPN伝送基礎データの無断複製等から保護することができる。

【0103】図12に示すように、コンパクトフラッシュ400は、PDA400のOSが認識できる領域411と、PDA400のOSが認識できない領域412にパーティションが分けられている。具体的には領域411はFATが存在するが、領域412はhiddenFATとしてパーティションを分割すればよい。領域412に図6に示すVPNデータ412dおよびこれを用いてVPNサーバとの間でVPN通信を行うVPNプログラム412vを、予め定めたデータフォーマットで記録しておく。領域412はPDA400のOSが通常のファイルシステムのデータフォーマットとは異なるデータフォーマットで記憶されているので、領域411にこの領域412に記録されたプログラムを起動する起動プログラム412aが記録されている。

【0104】かかる起動プログラム411aおよびVPNプログラム412vによるデータ処理を図13を用いて説明する。

【0105】まず操作者は、コンパクトフラッシュ433aをCFスロット433に挿入する。CPU423は、ROM425に格納されたOSに基づいてCFスロット433にコンパクトフラッシュが挿入されたか否かを判断しており（図13ステップS101）、挿入があるとコンパクトフラッシュ433aに自動実行のための定義ファイルを読み出す（ステップS105）。この場合、図12に示すように、定義ファイル411bをコンパクトフラッシュから読み出す。定義ファイル411bには、領域411に記憶された起動プログラム411a

を実行する命令が記載されており（図示せず）、CPU423は、起動プログラム411aをRAM427にロードする（ステップS107）。これにより、起動プログラム411aによる処理が実行される。

【0106】CPU423は起動プログラム411aに基づき、パスワード入力画面を液晶表示部430に表示する（ステップS109）。かかる表示がなされると、操作者はパスワードを入力部428から入力する。CPU423はパスワード入力があったか否かを判断しており（ステップS111）、パスワード入力があると、領域412に記憶されているVPNプログラム412vを読み出す（ステップS115）。領域412は、既に説明したように、PDA400のCPU423のOSのファイル管理システムとは異なる形式でデータ記録されているため、OSだけではデータを読み出すことはできない。しかし、起動プログラム411aは予め領域412に記憶されたデータを読み出すための情報を記憶しているのでかかる情報を用いて、VPNプログラム412vを読み出すことができる。CPU423は前記パスワードを用いて読みだしたVPNプログラム412vを復号化する（ステップS117）。CPU423は復号結果を参照して、復号ができるか否かを判断しており（ステップS119）、復号ができたと判断した場合には、復号化したVPNプログラム412vをRAM427にロードする（ステップS120）。なお、復号ができたか否かは、例えば、所定の位置に埋め込んでいた判断コードが復号化によって、読みとれるか否かを判断するようにすればよい。これにより、VPNプログラム412vによる処理が実行される。

【0107】CPU423は、VPNプログラム412vに基づき、VPNデータ412dを読み出す（ステップS121）。VPNデータ412dの読み出しについてはVPNプログラム412vの場合と同様である。CPU423は前記パスワードを用いて、読みだしたVPNデータ412dを復号化する（ステップS123）。CPU423は復号結果を参照して、復号ができるか否かを判断しており（ステップS125）、復号ができたと判断した場合には、復号化したVPNデータ412dをRAM427を用いて、VPNサーバとの間でVPNを構築する（ステップS127）。これ以降は、上記実施形態と同様に、図9に示す伝送処理が実行される。

【0108】なお、ステップS119にて、復号化ができない場合には、「正しいパスワードを入力してください」等のエラーメッセージを、表示してステップS109以下の処理を繰り返す。

【0109】また、ステップS125にて、復号化ができない場合には、「データが壊れているおそれがあります。管理者に連絡してください」等のエラーメッセージを表示して（ステップS128）、処理を終了する。

【0110】なお、上記実施形態と同様に、PDA400



0のCPU423は、OSに基づいて、CFスロット433に挿入されたコンパクトフラッシュ433aが取り外されたか否かを判断しており(図10に示す処理と同様に処理)、取り外されると、RAM427にロードされたプログラムおよびVPNデータを消去する。これにより、コンパクトフラッシュ433aをとり外した後は、当該PDAから許可なくVPNを構築されるおそれがない。

【0111】このようにコンパクトフラッシュを用いることにより、USB端子を有しないPDA機器をVPNクライアントとしてVPNを構築することができる。なお、OSの異なるコンピュータでもVPNクライアントとして構築できるように、領域411をさらに複数に分けてそれぞれに同じ起動プログラムを記憶しておき、いずれかの領域から起動プログラムが読み出されることにより、VPNプログラムが起動できるようにすればよい。例えば、コンパクトフラッシュの領域411<sub>1</sub>には、Palm(商標)用OS、領域411<sub>2</sub>には、windows(商標)CE用OS、領域411<sub>3</sub>には、・・・というように記憶しておけばよい。

【0112】また、この例では、PDAをVPNクライアントとする場合について説明したが、その他ノートパソコンなどの携帯端末についても同様に適用できる。

【0113】なお、かかる携帯端末が一旦記憶したデータをハードディスク等の記録媒体に一旦記憶するような場合には、前記読み出されたVPNプログラムやVPNデータをメモリ上だけでなく、かかる記録媒体から消去するプログラムを前記CF等に記憶させておき、自動実行するようにすればよい。

【0114】なお、図13においては、コンパクトフラッシュがCFスロットに挿入されると、定義ファイルから起動プログラム411aを自動実行する場合について説明したが、操作者が起動プログラム411aを手動で実行することもできる。この場合、図13において、ステップS101、ステップS105の代わりに、起動プログラムの実行指令が与えられたか否かで判断すればよい。

【0115】なお、図7に示すVPN伝送基礎データにて、相手先サーバのIPアドレスに代えて、IPサブネットアドレスで指定するようにしてもよい。この場合、図9ステップS43にて、伝送先コンピュータのIPアドレスが、メモリ127に読み出されているVPN伝送基礎データの相手先サーバの属するIPサブネットアドレスと一致するか否かを判断すればよい。すなわち、その他ドメイン名などの相手先サーバを一意に特定できる相手先サーバ特定情報を用いることができる。

【0116】本実施形態においては、VPNサーバとVPNクライアントとの間のネットワークとして、インターネットを採用したが、これに限定されず、他のネットワークであっても、他のユーザに対する守秘性を保持で

きるという効果を奏する。

【0117】なお、記録媒体には、VPN基礎データを読み出すVPN処理プログラムを記録しない場合でも、VPN基礎データを前記領域412のようにVPNクライアントのOSが認識できない領域に格納するようにしてもよい。この場合、かかる読み出すためのプログラムは予めVPNクライアントに記憶しておけばよい。

【0118】また、本実施形態においては、通信プロトコルとしてTCP/IPを採用したが、他の通信プロトコルを採用してもよい。

【0119】本実施形態においては、図2に示す機能を実現する為に、CPUを用い、ソフトウェアによってこれを実現している。しかし、その一部もしくは全てを、ロジック回路等のハードウェアによって実現してもよい。

【0120】なお、プログラムの一部の処理をさらに、オペレーティングシステム(OS)にさせるようにしてもよい。

#### 【図面の簡単な説明】

【図1】本発明にかかるVPN伝送システムの概略を示す。

【図2】本発明にかかるVPN伝送システムの機能ブロック図である。

【図3】図2に示すVPNサーバ100をCPUを用いて実現したハードウェア構成の一例を示す図である。

【図4】VPN伝送基礎データのデータ構造を示す。

【図5】図2に示すVPNクライアント200をCPUを用いて実現したハードウェア構成の一例を示す図である。

【図6】図1に示すデータ伝送機器300をCPUを用いて実現したハードウェア構成の一例を示す図である。

【図7】VPN伝送基礎データのデータ構造を示す。

【図8】VPN構築処理を示すフローチャートである。

【図9】VPN伝送処理を示すフローチャートである。

【図10】VPN切断処理を示すフローチャートである。

【図11】PDAをVPNクライアントとする場合の、PDAのハードウェア構成の一例を示す図である。

【図12】コンパクトフラッシュ433aのデータ管理方法を説明するための図である。

【図13】VPNデータ読み出し処理を示すフローチャートである。

【図14】従来のVPNシステムの概要を示す図である。

#### 【符号の説明】

23・・・CPU

27・・・メモリ

100・・・VPNサーバ

123・・・CPU

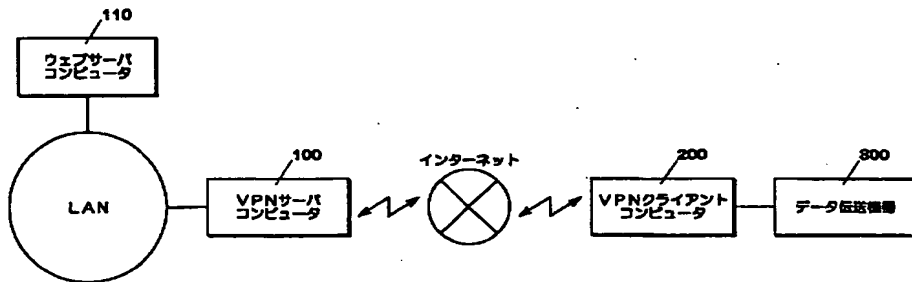
127・・・メモリ

200・・・VPNクライアント  
223・・・CPU

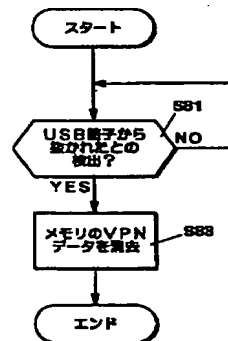
227・・・メモリ  
300・・・データ接続機器

【図1】

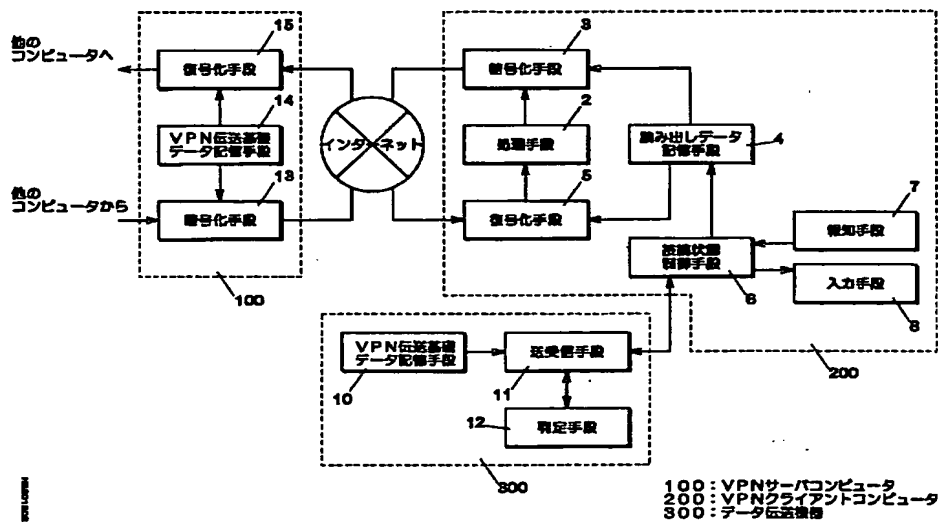
【図10】



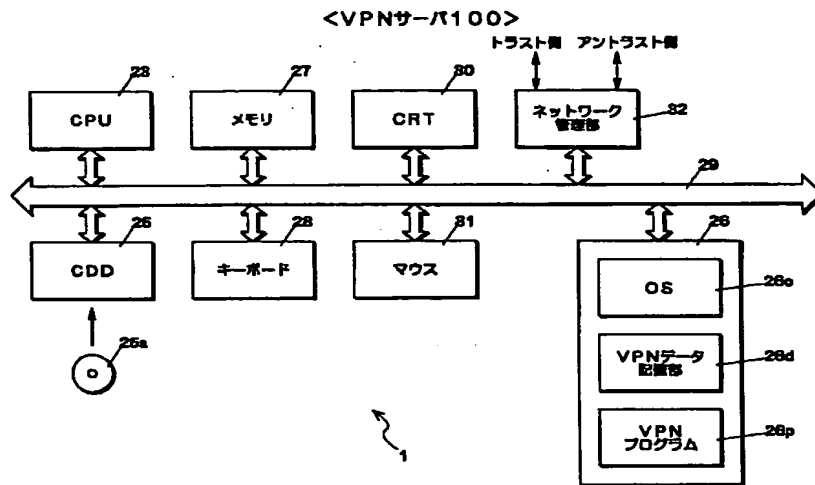
&lt;VPN切断処理&gt;



【図2】



【図3】



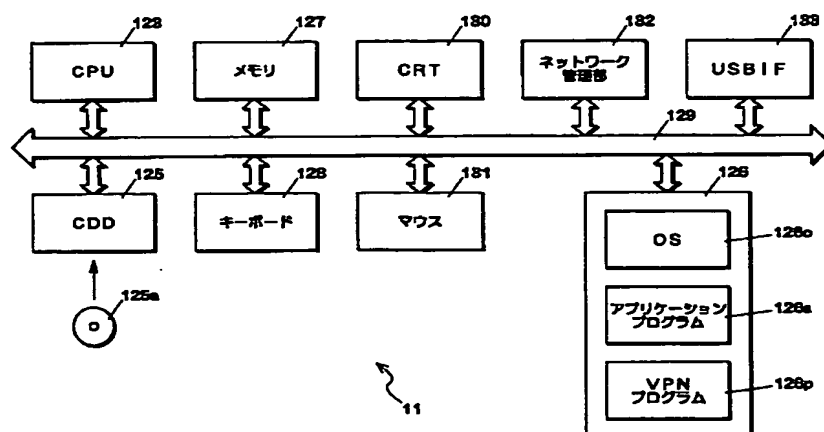
【図4】

**<VPNデータ記憶部>**

| VPNクライアント<br>識別子 | VPNサーバ<br>識別子 | VPN<br>暗号化方式 | VPN<br>暗号化キー | VPN<br>暗号化キー | 暗号VPNクライアント<br>IPアドレス |
|------------------|---------------|--------------|--------------|--------------|-----------------------|
| AC101            | AS105         | XXX1         | 595XXX5      | 325YYY7      | △△△                   |
| KC203            | KS109         | XXX2         | 805XXX3      | 986YYY2      |                       |
| PC301            | PS203         | XXX1         | 408XXX7      | 666YYY1      |                       |
|                  |               |              |              |              |                       |

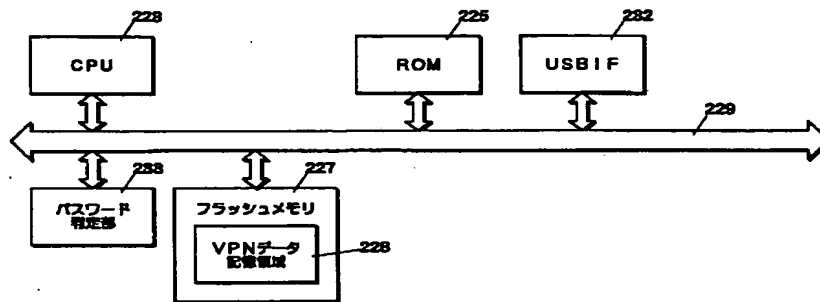
【図5】

**<VPNクライアント>**



【図6】

## &lt;データ伝送装置300&gt;



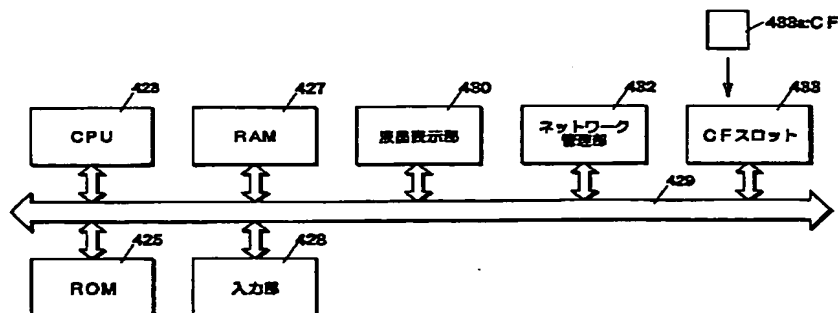
【図7】

## &lt;VPNデータ記憶領域&gt;

|               |             |
|---------------|-------------|
| ユーザID         | XX501       |
| パスワード         | *105010     |
| 使用期限          | 2001/12/31  |
| VPNサーバのIPアドレス | 202.XXX.YYY |
| 相手先サーバのIPアドレス | 202.XXX.XXX |
| VPN暗号化方式      | XXX1        |
| VPN暗号化キー      | 595XXX5     |
| VPN復号化キー      | 325YYY7     |
| VPNクライアント識別子  | AC101       |
| VPNサーバ識別子     | AS105       |

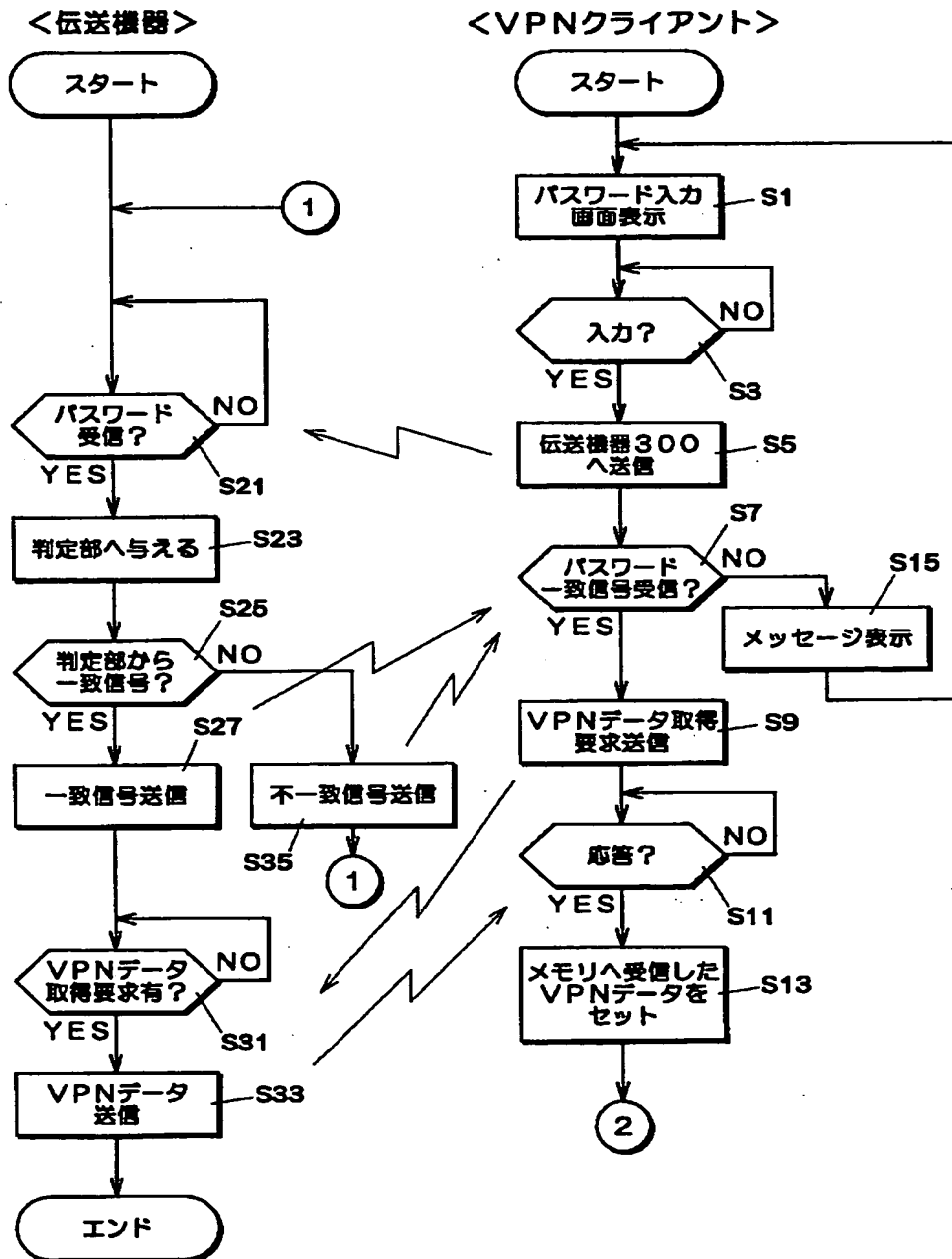
【図11】

## &lt;PDA&gt;



【図8】

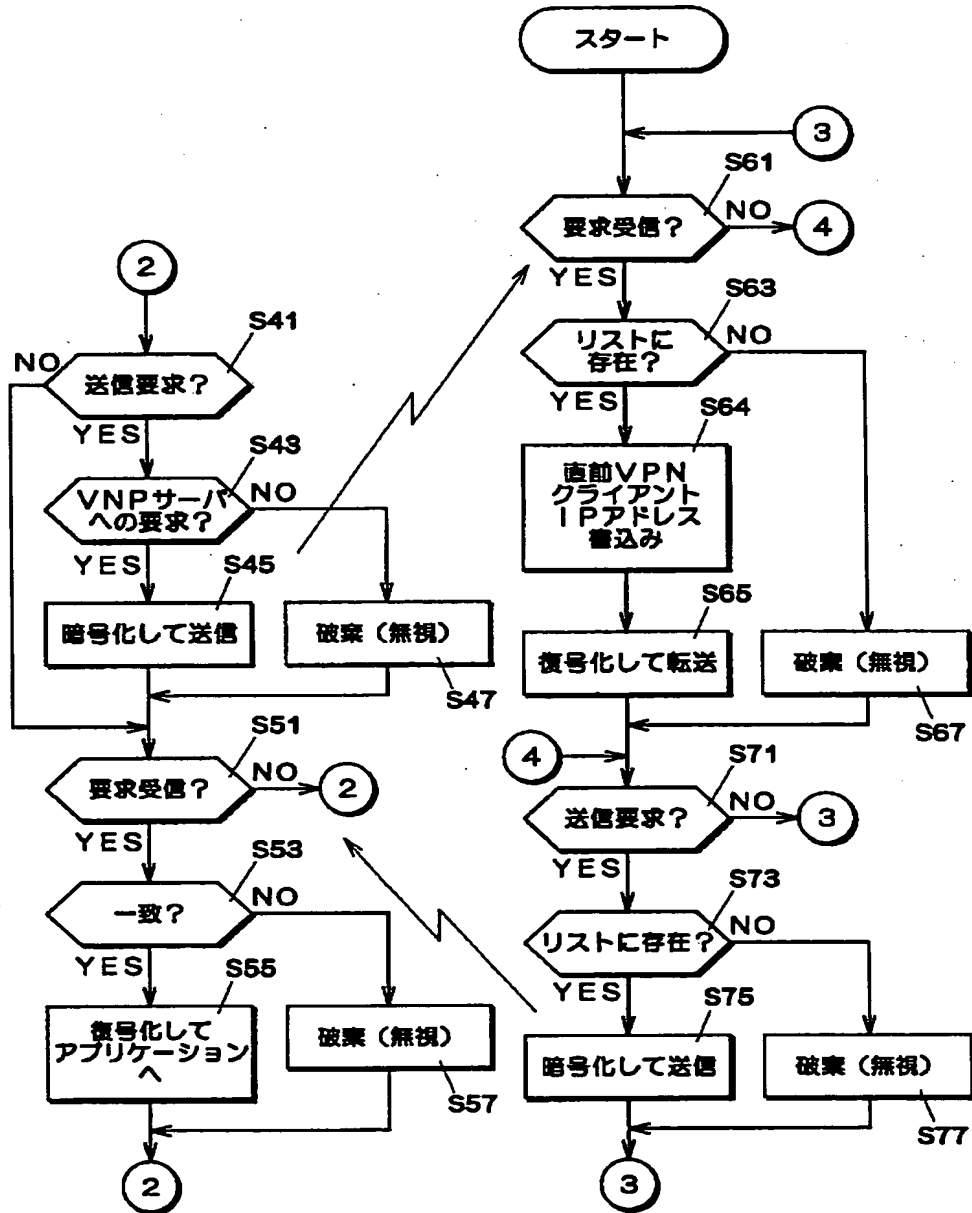
## &lt;VPN構築処理&gt;



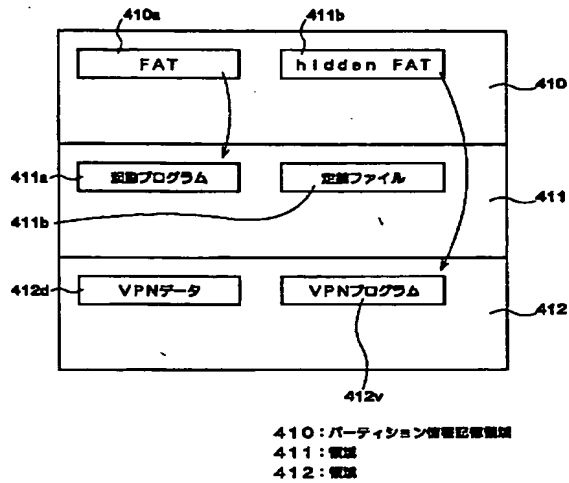
【図9】

## &lt;VPNクライアント&gt;

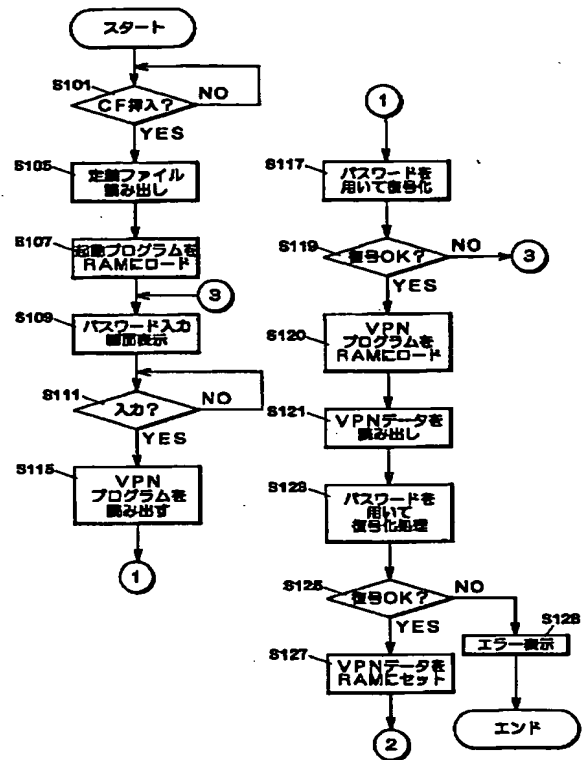
## &lt;VPNサーバ&gt;



【図12】

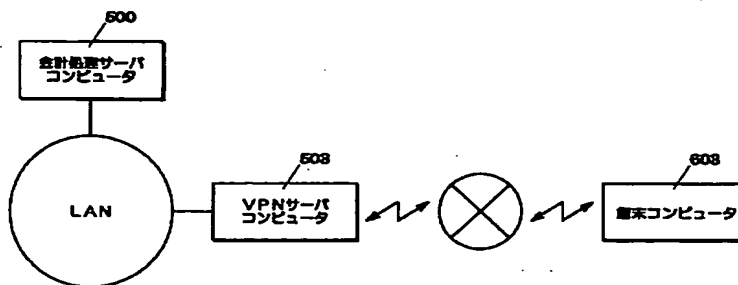


【図13】



【図14】

&lt;従来技術&gt;



フロントページの続き

(72) 発明者 柴山 裕子  
東京都新宿区西新宿三丁目19番2号 東日  
本電信電話株式会社内

(72) 発明者 岡田 健一  
大阪府大阪市中央区南本町2丁目4番16号  
株式会社日立システムアンドサービス内

(72) 発明者 小坂 達也  
東京都新宿区西新宿三丁目19番2号 東日  
本電信電話株式会社内  
(72) 発明者 源田 浩一  
東京都新宿区西新宿三丁目19番2号 東日  
本電信電話株式会社内

(72) 発明者 植野 圭二  
大阪府大阪市中央区内本町2丁目4番16号  
株式会社日立システムアンドサービス内  
F ターム (参考) 5B085 AA01 AE00 AE29 BE01 BG07  
5J104 AA07 AA16 EA04 EA16 EA26  
KA01 NA02 NA05 PA07